

**BRENIN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

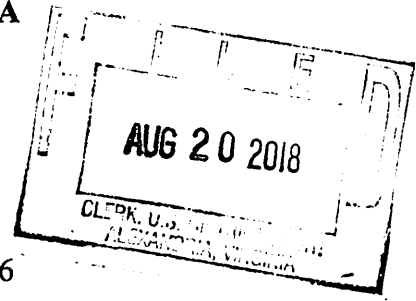
UNITED STATES OF AMERICA

v.

BRENDYN J. ANDREW,

Defendant.

No. 1:18-MJ-396



**AFFIDAVIT IN SUPPORT OF A
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Special Agent Daniel Overstreet, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Secret Service ("USSS"), and have been since on or about January 18, 2017. I successfully completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Program as well as the Special Agent Training Course at the James J. Rowley Training Center. In my training, I received specialized instruction in white-collar and computer-based crimes. Additionally, I am currently assigned to the National Capital Region Fraud Task Force. As such, I have participated in numerous white-collar investigations involving computers, to include wire fraud, bank fraud, and identity theft.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States, including 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1029 (Access Device Crimes), 1343 (Wire Fraud), 1344 (Bank Fraud), and 1349 (Fraud Conspiracy). I am also authorized to execute warrants issued under the authority of the United States.

3. The facts and information contained in this Affidavit are based upon my training and experience, personal knowledge, and observations during the course of this investigation, as well as the observations of other law enforcement officers involved in this investigation. This Affidavit contains only the information necessary to support probable cause, and it is not intended to include each and every fact and matter observed by me or known to the government.

4. This Affidavit is submitted in support of a Criminal Complaint and Arrest Warrant charging **BRENDYN ANDREW** with conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349. As set forth below, based on the government's investigation, there is probable cause to believe that, within the Eastern District of Virginia and elsewhere, **ANDREW** and at least one other individual knowingly and voluntarily joined together with each other and agreed to execute (or attempt to execute) a scheme or artifice to defraud financial institutions and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, those financial institutions, by means of false and fraudulent pretenses, representations, and promises, and they did so by unlawfully acquiring, possessing, and using credit or debit card numbers (*i.e.*, payment card numbers), as well as the personally identifiable information of other individuals, and then utilizing those misappropriated payment card numbers to fraudulently obtain goods, services, and money.

PROBABLE CAUSE

A. Overview of the Conspiracy Under Investigation

5. Since in or around July 2017, agents with USSS, the Federal Bureau of Investigation ("FBI"), the Arlington County Police Department ("ACPD"), and the Montgomery County Police Department ("MCPD") have been investigating the use of stolen payment card numbers and personally identifiable information ("PII") to fraudulently obtain goods, services,

and money from retailers within the Eastern District of Virginia and elsewhere.

6. It is common knowledge that financial institutions issue payment cards, such as credit and debit cards, to accountholders for their legitimate use in accessing the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of the issuing financial institution. These payment cards contain a magnetic strip that stores account data, such as the payment card number and any associated personal identification number, security code, or expiration date. It is also widely known that financial institutions maintain certain PII for each accountholder, which can include name, address, telephone number, email address, date of birth, place of birth, mother's maiden name, and account security codes, and this PII is associated with the accountholder's payment card number.

7. In my training and experience, criminals use a variety of schemes to steal payment card data and the associated accountholder's PII, which can then be re-sold or otherwise made available to other criminals. For example, stolen payment card data and PII can be obtained through the Internet using various technologies to provide the criminal with anonymity, including, for example, "The Onion Router" browser software, which is more commonly referred to as Tor. Tor software conceals an Internet user's location and online communications by encrypting the data in layers and routing it through an overlay network consisting of thousands of randomly selected relays.

8. In my training and experience, once the criminal has acquired the stolen payment card data and PII, the next step frequently is for the criminal to use the stolen payment card data and PII to conduct fraudulent transactions, which can include making fraudulent purchases through the Internet. I also know that another method for making fraudulent purchases using stolen payment card data and PII is to encode the stolen payment card data onto the magnetic

strips of physical cards. These re-encoded cards are then compatible with point-of-sale systems, and a criminal can swipe the card containing the stolen payment card information to conduct fraudulent transactions. In my training and experience, this scheme, in which a criminal conducts fraudulent transactions to obtain goods, services, or money using stolen payment card data and the associated accountholder's PII, is known as "carding."

9. I also know that the carding conspiracy described herein has victimized a number of financial institutions, and I know that at the time of the criminal conduct at least the following financial institutions were insured by the Federal Deposit Insurance Corporation: Bank of America, Barclays Bank, BB&T Bank, Capital One Bank, CitiBank, JP Morgan Chase Bank, PNC Bank, TD Bank, U.S. Bank, and Wells Fargo Bank. I also know that at the time of the criminal conduct at least the following financial institution was insured by the National Credit Union Administration: Navy Federal Credit Union.

B. Arrest of BRENDYN ANDREW on or about July 6, 2017

10. On or about July 6, 2017, ACPD officers responded to NOVA Armory, a firearms and accessories retailer located in Arlington, Virginia, within the Eastern District of Virginia, for a report of an individual attempting to pick up a 50-round ammunition drum. According to a NOVA Armory representative, this item had been purchased through the Internet using a stolen credit card number.

11. ACPD officers learned from a NOVA Armory employee that the aforementioned online purchase had been made through the Internet on or about June 22, 2017, utilizing a Citibank credit card number with the last four digits of 4183 (hereinafter "Citibank Card 4183"). Law enforcement determined that Citibank Card 4183 had been used to place two other NOVA Armory orders through the Internet on or about June 22, 2017. Those online orders involved the

purchase of ammunition. It appears that all of these purchases were fraudulent for the following reasons:

a. The NOVA Armory employee informed ACPD officers that he had identified the accountholder for Citibank Card 4183. An ACPD officer contacted this individual, identified herein as R.E., and learned that Citibank informed R.E. on or about June 24, 2017, that potentially fraudulent activity was associated with the Citibank Card 4183 and R.E. thereafter closed the account.

b. The contact information provided to NOVA Armory for all three purchases did not match R.E.'s contact information; instead, the information provided included the name "BRENDYN ANDREW" and telephone number (xxx) xxx-3105.

12. While on scene at the NOVA Armory on or about July 6, 2017, an individual later identified as **ANDREW** arrived at NOVA Armory in a vehicle bearing Maryland license plates that law enforcement determined was registered to **ANDREW**. **ANDREW** was observed attempting to claim the items that were purchased online using Citibank Card 4183. At that point, ACPD officers placed **ANDREW** under arrest.

13. ACPD officers conducted a search of **ANDREW** incident to arrest. Among other items located on **ANDREW**'s person was an iPhone 7, a New York driver's license bearing **ANDREW**'s photograph but the name Brian Hosier, a Navy Federal Credit Union debit card with the last four digits of 8751 bearing the name Brian Hosier (hereinafter "Navy Federal Card 8751"), and a Navy Federal Credit Union member access card with the last four digits of 9318 bearing the name "Brian Hosier" (hereinafter "Navy Federal Card 9318").

14. ACPD officers later determined that Navy Federal Card 8751 had been re-encoded with a Bank of America credit card number ending in 0666 (hereinafter "Bank of

America Card 0666"). ACPD officers contacted the true accountholder associated with Bank of America Card 0666, hereinafter referred to as J.C., who confirmed the card had been compromised and fraudulently used.

15. Subsequent to his arrest, ACPD officers notified **ANDREW** of his *Miranda* rights, and **ANDREW** stated that he understood his rights and voluntarily agreed to speak with law enforcement. During the ensuing interview, **ANDREW** admitted that he purchased one of the items that he was attempting to pick up at NOVA Armory, a 50-round ammunition drum, but he denied purchasing the other two items. **ANDREW** also indicated the following during the interview:

- a. that he purchased the ammunition drum from an anonymous third party through the Internet;
- b. that he sometimes used Tor to browse the Internet anonymously;
- c. he paid the third party using bitcoin, but he did not know how the third party paid NOVA Armory for the item;
- d. that his girlfriend (hereinafter "Co-conspirator 1") had also been involved with the purchase;
- e. that he utilized his personal contact information to make the purchase; and
- f. that his email address was xxxxxxxx03@gmail.com and his telephone number was (xxx) xxx-3105.

C. Search of **ANDREW's vehicle on or about July 7, 2017**

16. On or about July 7, 2017, pursuant to a search warrant issued by a magistrate of the Commonwealth of Virginia, ACPD officers conducted a search of the vehicle registered to **ANDREW** that he had arrived in at NOVA Armory.

17. During the search of the vehicle, ACPD officers discovered, among other things, four payment processor account activity statements showing account activity from vending devices VJ100143353 and VJ100143357 and associated payment processing terminals T0758377 and T0740295 and listing a corresponding Bank of America account number with the last four digits of 3511 (hereinafter “Bank of America Account 3511”). Although the payment processor account summaries listed the same Bank of America Account 3511, they identified various customer names, including **BRENDYN ANDREW**, Vending Delights, and Snack Standard Corp.

18. ACPD officers also discovered in the vehicle a Bank of America receipt for an account number with the last four digits of 7373 (hereinafter “Bank of America Account 7373”) in the name Brian Hosier doing business as Hosier Kicks Vending. A business-entity records search revealed that Hosier Kicks Vending was incorporated in Maryland on or about March 28, 2017, by an individual using the name Brian Hosier. The articles of incorporation listed a New York address for Brian Hosier as well as a business address in Gaithersburg, Maryland. Upon further investigation, law enforcement determined that Brian Hosier was not a real person, and instead was a fictional identity used by **ANDREW**. Law enforcement also determined that the listed Gaithersburg address was the residence of Co-conspirator 1’s parents. Law enforcement officers also determined that Co-conspirator 1 had at times used the listed Gaithersburg address as her residence address.

D. Search of ANDREW’s iPhone 7 on or about July 7, 2017

19. On or about July 7, 2017, pursuant to a search warrant issued by a magistrate of the Commonwealth of Virginia, ACPD conducted a search of the contents of the iPhone 7 seized from **ANDREW** at the time of his arrest. That search revealed that it was associated with

telephone number (xxx) xxx-3105, which **ANDREW** admitted was his and, as described above, was the telephone number utilized to make the suspicious purchases from NOVA Armory.

20. A search of the iPhone 7's notes application resulted in the discovery of more than 300 stored payment card numbers. Many of these payment card numbers were accompanied by security data and PII for what appeared to be the associated accountholder. The iPhone's notes application also contained financial information and PII for the "Brian Hosier" identity. Law enforcement officers also discovered a note dated on or about June 4, 2017, entitled "Things to do with \$," which stated, among other things, "\$1600 allocated for cc readers/skimers." In my training and experience, I have reason to believe that "cc readers/skimers" refers to two types of devices used to obtain payment card information from the magnetic strip of payment cards when they are swiped. In particular, I know that "skimers" are devices that can be installed within legitimate electronic payment mechanisms in order to steal payment card information.

21. During the search of the iPhone 7 text messaging application, ACPD officers uncovered a series of text messages exchanged on or about June 5, 2017, with an unknown individual. Among those communications were messages from the iPhone 7 to the unknown individual that appeared to be an attempt to recruit the unknown individual to use a skimmer at the unknown individual's place of employment to obtain payment card information for **ANDREW**.

22. Further review of the text messaging application resulted in law enforcement officers' discovery of numerous text messages containing payment card information received from Co-conspirator 1. For example, the iPhone 7 contained a text message received from Co-conspirator 1 containing R.E.'s Citibank Card 4183 and associated PII. That text message was

received on or about June 22, 2017, which was the same day the suspicious purchase from NOVA Armory was made through the Internet using R.E.'s Citibank Card 4183. The text message also contained the payment card information for a CitiBank payment card with the last four digits of 7450, along with PII, which is believed to correspond to a payment card belonging to a CitiBank accountholder identified herein as C.Y.

23. ACPD's examination of the iPhone 7 also uncovered evidence that on or about June 22, 2017, the iPhone 7's Internet browser was utilized to make the aforementioned purchase from NOVA Armory at a time when the iPhone 7 was connected to a wireless network identified as "ANDREW-2."

E. Search of ANDREW's Residence on or about July 31, 2017

24. On or about July 10, 2017, ACPD officers traveled to a residence in Rockville, Maryland, that was believed to be **BRENDYN ANDREW's** residence because law enforcement determined it was listed on **ANDREW's** Maryland driver's license and vehicle registration. While standing directly in front of this location, ACPD officers scanned available wireless network connections, and the wireless network "ANDREW-2" appeared for selection.

25. Thus, on or about July 31, 2017, pursuant to a premises search warrant issued by an associate judge of the State of Maryland, law enforcement officers, including MCPD and ACPD officers and USSS Special Agents, conducted a search of the aforementioned residence in Rockville, Maryland.

26. During the premises search, law enforcement officers discovered 33 blank payment cards in a bedroom. The cards had black magnetic strips, but nothing was printed on the front or rear of the cards. Upon further examination, law enforcement officers discovered that the payment cards were encoded with payment card numbers that are believed to be stolen.

27. Law enforcement officers also found an Apple MacBook computer among other electronic devices in the same bedroom. When the computer was recovered, it was on and its screen was visible to law enforcement. On that screen was an icon that law enforcement officers recognized as the icon for Tor, the anonymous browsing software that **ANDREW** had referenced in the interview with ACPD officers described above.

28. Law enforcement officers also recovered certain documents and contracts from the bedroom that indicated that a particular payment processing company would provide merchant services to a business entity identified as Creative Vending for a vending machine located at an address in Silver Spring, Maryland. The documents listed Co-conspirator 1 as the owner of Creative Vending and were signed using her name. However, a subsequent business-entity records search revealed that there is not a company incorporated in Maryland with the name Creative Vending and listing Co-conspirator 1 as an owner. Another document authorized the electronic transfer of funds to a Bank of America account number with the last four digits of 6817 (hereinafter "Bank of America Account 6817") listed in Co-conspirator 1's name.

29. Also recovered within the bedroom was a full-size snack vending machine with an installed payment processing terminal capable of processing payment card purchases. Subsequent investigation determined that between on or about December 7, 2016, and February 28, 2017, **ANDREW** and the entity Snack Standard Corp. maintained a contractual relationship with USA Technologies, Inc., a payment processing company, for the electronic processing of payment card transactions through the terminal found in **ANDREW**'s bedroom. According to USA Technologies, between January and February 2017, **ANDREW** received approximately \$75,000 under the contract for transactions processed through the terminal. Further investigation also showed that between on or about March 1, 2017, and April 1, 2017, USA Technologies

provided similar processing services for the same terminal to Brian Hosier and the entity Vending Delights. USA Technologies reportedly terminated both contracts after discovering suspicious account activity, which included multiple transactions in identical amounts, charged to the same credit card, and occurring less than a minute apart. Examples of suspicious transactions include the following:

a. On or about February 19, 2017, a Capital One payment card ending 2020 (hereinafter “Capital One Card 2020”) was processed through the terminal approximately 13 times by Snack Standard Corp, for charges totaling approximately \$1,746.29.

b. On or about that same day, another Capital One payment card ending 7457 (hereinafter “Capital One Card 7457”) was processed through the terminal approximately 14 times by Snack Standard Corp., for charges totaling approximately \$1,880.62.

c. On or about March 14, 2017, a Navy Federal Credit Union payment card ending 1263 (hereinafter “Navy Federal Card 1263”) was processed through the snack machine terminal approximately six times by Vending Delights, for charges totaling approximately \$3,000.

30. There is reason to believe that the bedroom where law enforcement located the items described in paragraphs 26 through 29 above was **ANDREW**’s and that he shared it with Co-conspirator 1 because law enforcement officers also found various identifying documents among other personal effects within the bedroom. For example, officers discovered a U.S. passport containing **ANDREW**’s photograph and PII in a bedroom drawer, and they discovered a Social Security card bearing Co-conspirator 1’s name and PII in a bedroom closet.

F. Search of ANDREW's Apple MacBook on or about August 1, 2017

31. On or about August 1, 2017, pursuant to a search warrant issued by a magistrate of the Commonwealth of Virginia, ACPD officers conducted a search of the contents of the Apple MacBook found in ANDREW's bedroom.

32. During the search, they discovered files on the computer that were associated with the email account xxxxxxxx03@gmail.com, which, as described above, was the same email account that ANDREW previously admitted to using when he placed the NOVA Armory order through the Internet. For example, ACPD officers discovered two emails stored within the computer, dated on or about September 15, 2016, and February 3, 2017, and addressed to the xxxxxxxx03@gmail.com email account, that contained what law enforcement officers recognized to be payment card numbers.

G. Search of xxxxxxxx03@gmail.com on or about August 8, 2017

33. On or about August 8, 2017, pursuant to a search warrant issued by a magistrate of the Commonwealth of Virginia, ACPD officers obtained from the service provider the subscriber information, activity logs, and contents of communications associated with the xxxxxxxx03@gmail.com email account.

34. Law enforcement officers thereafter conducted a search of the contents of the xxxxxxxx03@gmail.com email account and discovered numerous emails indicating that ANDREW utilized and controlled the xxxxxxxx03@gmail.com email account, including the following examples:

- a. an email dated on or about October 29, 2015, sent from xxxxxxxx03@gmail.com to xxxxxxxx03@gmail.com, containing a picture of ANDREW; and

b. an email dated on or about July 3, 2016, sent from xxxxxxxx03@gmail.com to xxxxxxxx03@gmail.com with the subject line "Here," containing a photograph of a U.S. Treasury check dated on or about July 1, 2016, and bearing **ANDREW**'s name.

35. ACPD's search of the xxxxxxxx03@gmail.com email account also resulted in the discovery of evidence relating to the acquisition, possession, and use of stolen credit card information during and in relation to a scheme to fraudulently obtain goods, services, and money, including the following:

a. an email that xxxxxxxx03@gmail.com received on or about February 11, 2017, with the subject line "-10" and containing ten payment card numbers;

b. an email received by xxxxxxxx03@gmail.com on or about April 8, 2017, with the subject line "Cc" and containing 39 payment card numbers;

c. an email received by xxxxxxxx03@gmail.com on or about April 9, 2017, with the subject line "Cc-7" and containing 21 payment card numbers;

d. an email received by xxxxxxxx03@gmail.com on or about May 24, 2017, with the subject line "cc" and containing five payment card numbers; and

e. email messages received by xxxxxxxx03@gmail.com on or about June 22, 2017, containing confirmations from NOVA Armory of the online purchases using Citibank Card 4183.

H. Arrest of BRENDYN ANDREW on or about June 11, 2018

36. On or about June 11, 2018, Montgomery County Police Department ("MCPD") responded to a tattoo parlor in Silver Spring, Maryland, for a report of an individual attempting to use a stolen credit card. When officers arrived, they learned that the individual, identified as


ANDREW, had attempted to purchase a tattoo with a Capital One credit card number ending 4537 (hereinafter "Capital One Card 4537"). Through their investigation, MCPD officers determined that Capital One Card 4537 actually belonged to an individual, identified herein as T.W., who was the true accountholder, and it had been stolen earlier that same day. At that point, **ANDREW** was placed under arrest.


37. MCPD officers conducted a search of **ANDREW** incident to arrest. Among other items located on **ANDREW**'s person was Capital One Card 4537. In addition, at the time of his arrest, **ANDREW** was in possession of a backpack, within which officers discovered a Verifone card reader and 13 receipts for purchases apparently made with the card reader.

CONCLUSION

38. In sum, based on the facts set forth in this Affidavit, I submit that there is probable cause to believe that **BRENDYN ANDREW** and at least one other individual did conspire to commit bank fraud, in violation of Title 18, U.S. Code, Section 1349. I therefore respectfully request the issuance of an Arrest Warrant for **BRENDYN ANDREW**.

Respectfully Submitted,


Daniel Overstreet
Special Agent
United States Secret Service

Subscribed and sworn to before me
this 20 day of August, 2018 /s/ Theresa Carroll Buchanan
 United States Magistrate Judge

The Honorable Theresa Carroll Buchanan
United States Magistrate Judge

Alexandria, Virginia